ST&IC: Illinois' Fusion Center

ST&IC: Illinois' Fusion Center

Illinois' Statewide Terrorism & Intelligence Center (ST&IC) serves the criminal justice and private/non-governmental/public sector communities as a centralized repository for the collection, analysis and dissemination of homeland security information. ST&IC was first constructed after 9/11 as the Counter-Terrorism centric center for the State of Illinois. It has matured and expanded into a successful 24/7 All Crimes approach for actionable information to support efforts to anticipate, identify, prevent and/or monitor criminal activity. ST&IC continues to evolve in its mission to collect, compile, analyze and disseminate information to and from these communities. Fused data products are compiled from a variety of sources to include threats, suspicious activities, public safety, law enforcement, public health, social services and public works information.

Fusion Center Defined:

-A center established by State and local governments designed to co-ordinate the gathering, analysis and dissemination of law enforcement, public safety, and terrorism information"

- A collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity.

- DOJ/DHS Fusion Center Guidelines, July 25, 2005.

The current mission of the Statewide Terrorism & Intelligence Center is to provide timely, effective, and actionable intelligence/information to local, state and federal law enforcement and private sector partners in order to enhance public safety, facilitate communication between agencies, and provide support in the fight against terrorism and criminal activity.

Considered collectively as a team yet in spirit diversely talented, ST&IC personnel are the essence of the Center. Their work requires them to be diligent, methodical and resourceful in their analytical approach to research,

evaluate and disseminate critical preventative, preparedness and response/recovery information. This data is cross-referenced with sustained warehouse information for outcomes and products compiled for the protection of the citizens and businesses of Illinois and beyond.

Initiatives

ST&IC Expansion

The fusion center continues expansion to include disciplines of contingency planning (NG), public health, fire and Geographic Information Systems (GIS) analysis for action-oriented and value-added information for it clients and partners. These developments are currently underway and will provide diverse platforms of information gathering and exchange. The challenge for ST&IC is to fuse this sundry of information in methods that will provide utility and purpose for the recipients. This succession of additional components is an opportunity for Illinois to continue to be a vanguard of intelligence/information sharing.

ISA Program

One of ST&IC's goals is to promote mutually collaborative communications, working relationships, partnerships and information sharing between private and public sector entities.

The Infrastructure Security Awareness Program (ISA) is an on-going illustration of these efforts. The program was initiated in September 2004, and was designed as a cooperative engagement to share vital, For Official Use Only (FOUO) information and ensure timely dissemination of critical infrastructure protection guidance and intelligence with those who have a "need to know". It continues as an information exchange and communications platform among private sector professionals requiring and sharing homeland security awareness, prevention, response, mitigation and recovery information. The delivery tool for this information is through a Department of Homeland Security (DHS) Internet portal, Homeland Security Information Network (HSIN). Access will be granted to those individuals who have a "need to know" or use the information contained in the ISA portal for FOUO business activities. Members also have access 24/7 to ST&IC analytical staff who can address inquiries, record and research suspicious activities and/or share timely threat/event information.

Information housed on the HSIN portal is organized by the following categories: alerts, calendar of events/anniversaries, document library, situational awareness and a training calendar. Topical information can be posted, requested, reported, viewed and shared with other members.

Private Sector applicants having a vested interest in protecting critical assets and key resources are vital to the program's success. The information shared can be from physical security, asset protection, cybercrimes intrusion, threat, suspicious activities, operational, crisis management or emergency preparedness perspectives. Members can also

exchange applicable, critical "responsibility to inform" type information obtained within the corporate security and resiliency communities. After validation of application information, the PNG Committee Chairpersons and ST&IC Command review all applications and retain sole discretion of accepting or rejecting applicants. There is no fee to participate in this forum.

ISA Sub-Initiatives

HSIN (Homeland Security Information Network):

A communications protocol sponsored by the Department of Homeland Security (DHS) for information sharing and exchange with/among Private Sector entities in Illinois. Other communication tools have been used by the program (MS Groove) or considered but currently HSIN is the platform for the program. HSIN can also be used by each state to communicate with its federal, state and local law enforcement agencies as well as their private sector partners. DHS has established a separate site for each state.ST&IC would like the ability to either execute technology changes to HSIN (Illinois) itself or acquire a portal the fusion center could maintain for future requirement change requests.

HSIN Portal Training:

-Announcements - This appears on the first screen. Only items of heightened awareness will be posted here.

-Calendar - Special events/anniversary dates. Self enter any events not included on the calendar.

-Homeland Security - Post RFI/FYI informational

- RFI should be used if you ask information from the group. FYI is used as the discussion thread and STIC will post suspicious events here.

-Contacts - You can add your contact information below the FYI section.

-Info/Doc Sharing - This is where unclassified or FOUO documents are stored.

There are folders and subfolders created for each infrastructure sector to save information.

-Situational Awareness/COP - DHS provides information on ongoing events.

-Support – ST&IC will post information on upcoming training and service announcements. *Remember there is a search tool located in the top right corner of the screen that will help in locating information and documents.

-Setting Alerts - You can set the site to send you an e-mail every time new information is posted. Use the Announcement Section as an example: Left click on announcements - on the right hand side will be an action called

"Alert Me". Right click on Alert Me, and enter your e-mail address. You will need to this for each of the sections you want to be alerted on (i.e., Info/Doc Sharing, Collaboration, etc.)

Retail Theft Initiative

As part of the HSIN communications portal, an initiative was developed to support a joint partnership between law enforcement and shopping mall security in northern Illinois as a pilot project to share real time information regarding organized retail theft groups via the portal. This initiative was requested jointly by law enforcement and security entities as an opportunity to share timely information with their partners. DHS agreed after a period of time to make the appropriate technology changes to the system which would allow for the requested exchange through a separate screen to collect and share this information.

Monthly Intelligence Briefings

To meet the information sharing needs of the private sector, ST&IC began to conduct monthly "All Crimes" briefings at the "For Official Use Only" classification level in January 2008. Using web conferencing to conduct live meetings and presentations over the Internet, STIC is able to engage the private sector in a more efficient

information sharing/exchange manner.

Yearly Conference

Annual information sharing requirements summit were held in 2007 and 2008 with members of the Infrastructure Security Awareness (ISA) Program to discuss sharing timely, functional and serviceable information between ST&IC and its private sector members. These sessions were hosted by private sector companies in support of the ISA program and continued actions for information sharing and participation with Illinois' fusion center. An example of a recommendation that came from one of the summits was the monthly webinar intelligence briefing conducted by ST&IC with its private sector partners.

ISA Membership

Marketing of the program continues through formal, informal and one-on-one presentations/ meetings. Efforts are underway to research then engage private sector entities beyond the physical security/ asset protection sectors – with next steps to include resiliency, business continuity, resumption, contingency planning, crisis management and emergency management entities. These disciplines will bring into the program more diverse types of information sharing and actions. (On-going)

Changes to the ISA application are underway to include a non-disclosure agreement component to ensure proper use and safe-keeping of the information. (Under Legal Review)

A rejection policy for ISA member applicants that do not meet standards should be jointly established and uniformly reviewed and administered by the PNG Chairs and ST&IC Command. (Pending)

Critical Infrastructure Specialist Position

**(See detailed description)*

Types of information sharing with the Private Sector include:

Strategic
Sector Specific Threat Assessments, Intelligence Requirements, Intelligence Management and Trend Analysis

Operational
Major Events, Daily Briefings, All Hazards Reports and Daily Intelligence Notes

Tactical
On-scene Support, Routine Requests

Utility Crimes Task Force

Initiate a task force and partner with utility companies, law enforcement and the fusion center to address crimes committed against utility companies and their service personnel. Information sharing through a searchable database by location with a mapping function provides a repository for reported incidents. This repository is a way for the utility companies to either directly or indirectly have access to information provided by other utility company partners about past incidents for future proactive precautionary measures.. Analysis of this information could identify methods of operation (MO), targeted companies and safety initiatives. (Proposal for PNG Funding)